QKDP's Comparison Based upon Quantum Cryptography Rules

Abdulbast Abushgra
Computer Science & Engineering Department
University of Bridgeport
Bridgeport, USA
aabushgr@my.bridgeport.edu

Khaled Elleithy
Computer Science & Engineering Department
University of Bridgeport
Bridgeport, USA
elleithy@bridgeport.edu

***Abstract*—Quantum key distribution (QKD) is the future of the cryptography world. The QKD was invented to increase the security rate when exchanging a private key. Since 1984, several experimental attempts to design protocols have been developed based upon the rule of physics. These QKD protocols were represented by different algorithms with limited ability to stand up against quantum attacks. This paper evaluates the most functional QKD protocols in the cryptography field and explains every QKD protocol as well illustrates the features that were utilized in each protocol.**

Keywords- Quantum Key Distribution, Entanglement State, Polarization, Qubit, and Pauli matrices.

I. INTRODUCTION

The security of data exchange between multiple parties is considered to be an extremely risky procedure. A secured data exchange system must be designed for scientists, governments, foundations, and the entire population. In order to guarantee the transfer of secured data by multiple parties, the data must be encrypted with a key that can only be identified by the sender (Alice) and the receiver (Bob). This encryption key is usually created by the sender, and it is submitted to the receiver through various communication channels.

In classical cryptography, creating an encryption key is based on the complexity of the mathematical equations and the difficulty of solving these equations. R.L. Rivest, A. Shamir, and L. Adleman created the RSA [1], a well-known complex cryptanalysis algorithm. In addition, Shor's algorithm [2] is considered to be one of the more robust algorithms in the classical and quantum security. It uses powerful calculation derived from number factors to increase the level of difficulty needed to access the generated key. Occasionally, Shor's algorithm is used in the reconciliation and error correction phases.

In classical cryptography, the secret key can be created by either the sender alone, the sender and the receiver, or the third party. In complicated procedures, the secret key should only be used once. In addition, the key should be adapted in certain protocols where the key contains an extraordinary amount of bits that may equal the length of the plain text. A secured key will ensure a safe method of transferring information between parties. The more complex the secured key, the safer the information transfer. So classical cryptography is the process that occurs within an unexpected amount of time through the execution of complex mathematical sequences. As a result, the researchers must constantly strive to improve communication security.

II. QUANTUM KEY DISTRIBUTION PROTOCOLS

The QKD protocol is the mechanism used to create a secret key through the law of physics and based on the fundamentals of digital and photon measurements. Several protocols were introduced to demonstrate reliable QKD protocols. Some QKD protocols have a reasonable ability to be processed and have withstood quantum attacks. In addition, QKD protocols can be applied through a current security systems [3]. These QKD protocols were designed in different schemes, and some of these protocols required specific devices. The following section briefly explains some interesting QKD protocols.

A. The BB84 Protocol

In 1984, Charles H. Bennett and Gilles Brassard presented the first QKD protocol that depends on quantum mechanics. This protocol is called the BB84, and it utilizes the particularity of state polarization for creating the single qubit (Quantum Bit). The BB84 protocol employs two bases of measurements and four states of the photon polarization.

$$|\varphi\rangle = \alpha|0\rangle \pm \beta|1\rangle,$$
$$|\emptyset\rangle = \alpha|0\rangle \pm \beta|1\rangle.$$

In the history of quantum key distribution, there is no protocol similar to the BB84 protocol in the simplicity of the communication process. Although few researches have proven that the BB84 protocol is not secured, it is still theoretically used by several QKD protocols.

B. The B92 Protocol

In 1992, the B92 protocol was proposed by C. H. Bennett. The B92 protocol is similar to the BB84 protocol except the B92 protocol uses two non-orthogonal states rather than four states. The B92 protocol also is based on the Heisenberg's Uncertainty Principle [4]. The B92 protocol is explained as follows [5, 6]:

- Alice starts creating n random qubits through two bases (×, +) and two non-orthogonal states.

$$|0\rangle, |1\rangle,$$

$$|-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}, |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}.$$

- Bob measures the received qubits in random basis as shown below in Table (1):

TABLE 1. THE EXCHANGE AND THE MEASUREMENT IN THE B92 PROTOCOL.

Bob Bases	×			+		
Bob observed	↑	→	→	↖	↗	↗
Alice sent	↗	→	?	→	↗	?

- Bob communicates with Alice publically.
- Bob must identify uncertain measurements to Alice, and Alice must omit them.

The B92 protocol utilizes most of the BB84 scheme steps that are based upon the polarization of the states, but it takes a critical action when Bob measures Alice's qubits in two bases to produce two states.

C. The SARG04 Protocol

This protocol was introduced [7] by V. Scarani, A. Acin, G. Ribordy and N. Gisin in 2004. The SARG04 is similar to the BB84 protocol except in the reconciliation and correcting errors phase. This protocol has proved to be secure protocol against a Photon Number Splitting (PNS) attack. Based on current technology, a PNS attack is not likely to occur. The SARG04 protocol is as follows:

- Alice initiates random binary bits in non-orthogonal bases, and she submits the binary of qubits to Bob.
- Bob measures the upcoming qubits in random bases, and he only gains the right measurement if he uses the bases that match with her qubits.
- Alice announces Bob by two states; one state is that she already sent, and the other state is random states from other basis.

The above QKD protocol was designed to improve the BB84 protocol, and it provides an identical security to the BB84 protocol in ideal implementations. However, the SARG04 protocol is more secure when the PNS attack is presented.

D. The Coherent-One-Way Protocol

In 2008, the Coherent One Way (COW) protocol was presented by Nicolas Gisin, and other researchers. The COW protocol implements the secret key by the time of arrival measurements on the data line. The source, data, and monitoring lines are the sequential terms of the COW protocol [8]. Generally, the COW protocol's algorithm is summarized as follows [9]:

- Alice generates a string of bits that contains 0 and 1 with the probability of $(1 - f)/2$, as well as sequence of decoy bits with a probability of *f*.
- On the other hand, Bob measures the bits by two detectors: the first detector "DB" is for time and the second detector "DM2" is for security.
- Bob reveals the bits after the measurement, where the number of bits can be detected by DB, and the time of detections will be monitored by DM2.
- Alice reviews the sequences of bits and the detection time on the interferometer, and she is able to detect any eavesdropping on the submitted bits.
- Alice informs Bob that the bits are needed must be removed from the string bits on Bob's raw key.
- Bob extracts the bits that will generate the secret key.

E. The KMB09 Protocol

The KMB09 was announced [10] by Muhammad Khan and others in 2009. The KMB09 differs from the BB84 protocol and other QKD protocols by detecting the presence of eavesdroppers that use the calculation of the index transmission error rate (ITER) instead of quantum bit error rate (QBER). The participants utilize two bases (*e* and *f*) with all states of both bases, and each bit will be transmitted only when the participants use different bases. Basically, the KMB09 protocol's algorithm scheme works as follows:

- Alice initiates a string of random bits and assigns each single bit randomly into an index $i = 1, 2 \ldots N$.
- Alice sends the prepared sequential bits to Bob into one of the states (*e* or *f*).
- Bob utilizes the both states (*e*, *f*) to measure the upcoming qubits.
- Alice informs Bob publicly of the submitted indices *i*.
- Bob matches his measurements with Alice's indices, and he keeps the matched bits and announces to Alice about the interrupted bits.
- Alice and Bob must decide if the concluded secret key is eavesdropped by Eve when the error rate has high percentage or to keep the successful bits when the error rate is low.

Therefore, Alice and Bob are able to reject the measured states that have the same index.

F. The EPR Pair Paradox Protocol

In 1935, the EPR Pair Paradox was presented in one of the interesting papers by A. Einstein, B. Podolsky, and N. Rosen. The main notion of this paper [11] is to approve the certainty of entanglement elements. In 1991, Arther K. Ekert [5] came up with the EPR protocol based upon the previous theory. Ekerts' theory states that when a pair of entangled qubits are measured, both qubits will collapse. The EPR protocol is explained in steps

that will be between two communicators with ability to generate entangled qubits as follows:

- Alice and Bob should be able to receive one of the entangled qubits, regardless of the initial receiver.
- Alice and Bob measure the upcoming entangled qubits into a random sequence of bases that must be separated by both.
- Alice and Bob communicate publically to compare the measured qubits, where they keep the qubits that were measured into same basis, and they discard the others.

G. The Differential-Phase-Shifting Protocol

The Differential Phase Shifting (DPS) Protocol was presented [12] by Kyo Inoue, et al., in 2002. The main premise of the DPS protocol is based on splitting the photon into a Three-Beam splitter with equal ratio, and then the submitted photons are recombined into two modulated phases.

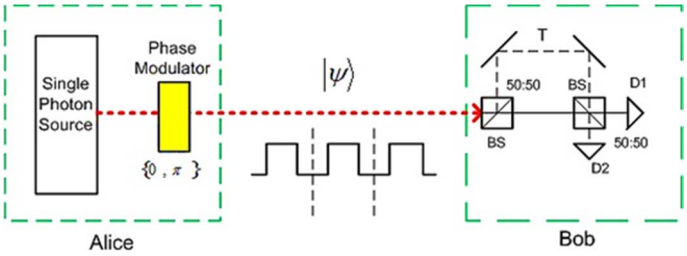

FIGURE (1). SCHEMATIC DIAGRAM OF DPS PROTOCOL.

Alice modulates random pulses of weak coherent states by {0, π} for each pulse. After that Bob measures the upcoming pulses by using photon detector D1 and detector D2, in which these detectors click based on the arrival photons in different phases [13]. Then Bob informs Alice about the time that was counted at detectors. The DPS protocol gives a robustness standing against a PNS attack.

H. The S13 Protocol

In 2013, S13 protocol [14] was introduced by Eduin H. Serna. This protocol was designed not to lose any information between the transfers of communication by two parties. The protocol's mechanism is based on a random seed and asymmetric cryptography that are processed in multiple exchanges. The One-Time-Pad is guaranteed to be secured, as long as the secret key is random and contains the same length of the plain text. Therefore, the S13 protocol was designed to match the One-Time-Pad by generating a secret key with zero losses. This protocol is similar to the BB84 protocol in quantum manipulations, however, it varies in using the private reconciliations, a Random Seed, and Asymmetric Cryptography.

I. The AK15 Protocol

The AK15 protocol [15] was presented in 2015 by A. Abushgra and K. Elleithy. The AK15 protocol employs the polarized n states into two bases, and it is based on the Heisenberg's Uncertainty Principle. Also, the functionality of the preparation of the AK15 protocol is based on the power of the matrix, in which the prepared qubits are inserted into sequential lower-triangle and upper-triangle. The upper-triangle is responsible to hold random qubits, and the lower-triangle is for the encrypted secret key that is needed to be shared between two participants. The AK15 protocol's scheme is described in multiple steps as follows:

- Alice initiates a communication into EPR channel to create an authentication key (many steps included [15]).
- The authentication key must have the encoding process through the quantum channel such as the size of the matrix, sorting rows, and the initiation time.
- Alice fills up the lower-triangle (data) and the upper-triangle (random qubits), and she resorts the rows based on the authentication key.
- Alice sends the sequence of qubit rows in identified time, known length, and its indices.
- Bob measures the upcoming qubits, and he knows the size of used matrix. He uses the parity cells to check if there were any interruptions or not.
- Bob makes a decision to accept the communication if the QBER is over 90%. If the QBER is below 90%, Bob can reject the communication and restart another one.

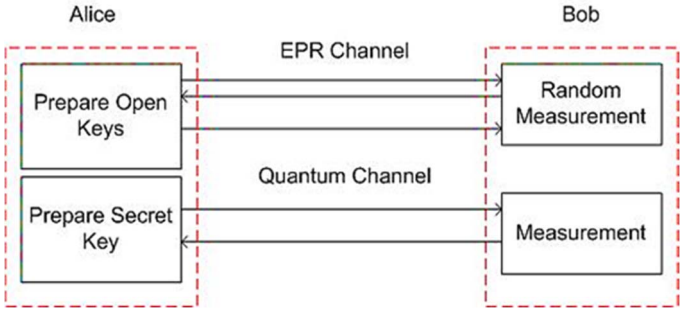

FIGURE (2) SHOWS THE GENERAL AK15 PROTOCOL SCHEME.

III. THE COMPARISONS OF QKD PROTOCOLS

The QKD protocols were compared based on the features of the protocol being secure or un-secure as follows in the Table (2). Most QKD protocols were classified based on the observables and quantum measurements, which make a decision to choose what kind of measuring and detecting devices will use. Using different states into the measurable channel will certainly determine the measurement system that each participant has to have. Also, Decoy states are mostly convenient to prevent some quantum attacks such as IRA.

Table [2] THE COMPARISON BETWEEN COMMON QKD PROTOCOLS.

Cases	*Quantum Key Distribution Protocols*								
	BB84	**B92**	**SARG04**	**COW**	**KMB09**	**EPR**	**DPS**	**S13**	**AK15**
Properties	Heisenberg	Heisenberg	Heisenberg	Entanglement	Heisenberg	Entanglement	Entanglement	Heisenberg	Heisenberg
Number of States	4 states	2 States	4 States	Time slots	2 states	Entangled 2 of photons	4 States	4 States	*n* states
Detection of presence	QBER	QBER	QBER	Break of coherence	ITER	Bell's inequality	Time-instance	Ran. Seed Asymmetric	QBER + Parity Cell
Polarization Situation	2 orthogonal	1 non-orthogonal	coded bits	No, using DPS	No	No	4 non-orthogonal	2 orthogonal	2 Orthogonal
Probability of each state	Various	50%	50%	equal	50%	equal	equal	Various	Various
Qubit case	DV	DV	DV	DV	DV	DV	DV	DV	DV
Classical channels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Decoy States	No	No	No	Yes	No	No	No	No	Yes
Sifting phase	Revealing Bases	Alice = 1 - Bob	Revealing non-orth. state	revealing the times 2k+1	determining the error rate	Bell's Inequality	No	Revealing Bases	No
Bell's inequality	No	No	No	No	No	Yes	No	No	Yes
PNS attack	Vulnerable	Vulnerable	It's better than BB84	Robust	Robust	N/A	Robust	N/A	Robust
IRUD attack	Vulnerable	Vulnerable	Vulnerable	Under Test	Under Test	Vulnerable	N/A	N/A	Robust
Beam-Splitting attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Vulnerable	Robust	N/A	Robust
Denial of Service attack	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Robust	N/A	N/A
Man-In-The-Middle attack	Vulnerable	Robust	Robust	Robust	Robust	Robust	Robust	N/A	Robust
IRA attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Bell's inequality	Robust	N/A	Robust

These information were collected from different resources (journals, articles and conference papers) and whole information and data above are based on either the original studies or the latest improvement. Also, this paper focused on just nine of the most famous protocols that will be the foundation of quantum computer world. Furthermore, some of the details have been received from the original publication where it was not studied more than one or two; On the other hand, others were had the details from different studies such as BB84, which has plenty of studies in different approaches.

According to the previous table, the classical channel is used mainly in the executing time of each protocol except the AK15 protocol. Moreover, correcting the errors that might happen naturally by environment or by eavesdropper is the core of the whole communication and exchanging data. Some quantum protocols just use the QBER, which is still an inaccurate correction system. Few of these protocols employ a strong algorithm to prevent any gaining to the submitted data by eavesdropper such COW, KMB09, and AK15 protocol.

IV. Conclusion

This paper identified a group of QKD protocols that are classified as the most practical and usable QKD protocols. These studied protocols were analyzed into a specific cryptographic field to show the robustness of each one of these protocols. The main point in this paper focused on the comparison between QKD protocols that are based on a technical side of cryptography. The study shows some QKD protocols that are reliable and secure against some quantum attacks but their devices are not available nowadays. On the other hand, other QKD protocols have the ability to be processed into a classical system but their security is still under test. Thus, the combination of physics features together with mathematics rules cover a huge gap between the classical and the quantum cryptography.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 26, pp. 96-99, 1983.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM journal on computing,* vol. 26, pp. 1484-1509, 1997.

[3] A. Abushgra and K. Elleithy, "Security of Quantum Key Distribution," 2015.

[4] M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocols: A survey," *International Journal of Universal Computer Sciences,* vol. 1, pp. 59-67, 2010.

[5] N. S. Yanofsky and M. A. Mannucci, *Quantum computing for computer scientists* vol. 20: Cambridge University Press Cambridge, 2008.

[6] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters,* vol. 68, p. 3121, 1992.

[7] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters,* vol. 92, p. 057901, 2004.

[8] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," *arXiv preprint quant-ph/0411022,* 2004.

[9] A. Khaleel, "Coherent one-way protocol: Design and simulation," in *Future Communication Networks (ICFCN), 2012 International Conference on*, 2012, pp. 170-174.

[10] M. M. Khan, M. Murphy, and A. Beige, "High error-rate quantum key distribution for long-distance communication," *New Journal of Physics,* vol. 11, p. 063043, 2009.

[11] N. Bohr, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review,* vol. 48, p. 696, 1935.

[12] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase-shift quantum key distribution," in *Photonics Asia 2002*, 2002, pp. 32-39.

[13] H. Singh, D. Gupta, A. Singh, P. S. Burvin, J. M. Esther, S. S. Shrimandal, R. B. Nadagoudar, R. B. Venkatapur, S. Himaja, and N. C.

[14] S. Reddy, "Quantum Key Distribution Protocols: A Review," *Journal of Computational Information Systems,* vol. 8, pp. 2839-2849, 2012.

[15] E. H. Serna, "Quantum Key Distribution from a random seed," *arXiv preprint arXiv:1311.1582,* 2013.

[16] A. Abushgra and K. Elleithy, "Initiated decoy states in quantum key distribution protocol by 3 ways channel," in *Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island*, 2015, pp. 1-5.